FS Policy 301-2, Email and Instant Messaging

Original Issue Date: December 2015
Last Review Date: August 2024
Next Review Date: August 2028

Executive Summary

Describes the requirements and procedures related to the use of electronic mail (email) and instant messaging (IM) technologies.

Purpose

Establishes Fiscal Service requirements regarding the use of email and IM by Fiscal Service employees and affiliates.

Scope

Applies to all Fiscal Service employees, including appointees of the Senior Executive Service. In the event of a specific policy conflict between the Master Labor Agreement and this Policy, the Master Labor Agreement is the controlling document for bargaining unit employees. This policy applies to all contractors, sub-contractors, financial agents, and fiscal agents who have access to Fiscal Service email and IM systems.

Cancellations

- FS Policy 301-2, Email and Instant Messaging March 2020

References

- OMB Memorandum M-07-16
- OMB Memorandum M-22-09
- Treasury Directive 87-04
- Treasury Directive Publication 15-71 – Treasury Security Manual
- Treasury Directive Publication 85-01 – Department of the Treasury Information Technology (IT) Security Program
- Internal Revenue Code Section (§) 6103
- Internal Revenue Service Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies
- Fiscal Service Baseline Security Requirements (BLSRs)
- Fiscal Service Policy 207-1, Employee Conduct

This policy supplements policies and requirements contained in the references cited above.

Definitions

A. Affiliates: Individuals or groups, excluding Fiscal Service employees, who are performing work on behalf of Fiscal Service.

B. Bulk Email: Electronic mail messages sent to all Fiscal Service employees, all Fiscal Service employees working out of a specific office, or all employees of an area managed by a particular Assistant Commissioner.

C. Compromise: An act that impacts the confidentiality, integrity, and/or availability of information or an information system. This includes disclosing information to parties without a need to know, altering information without authorization to do so, or rendering information or an information system inaccessible from an alternate source.

D. Controlled Unclassified Information (CUI): Any information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify. Personally Identifiable Information (PII) falls under the data classification of CUI.

E. Controlled Unclassified Information (CUI) HIGH Risk Information: Any information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls and that poses a catastrophic risk to the Government's Mission Essential Functions if it is compromised. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify. Examples include: proprietary controlled business processes, FIPS 199 high information (which may or may not include PII), security architecture for critical systems, system security documentation for FIPS 199 high systems, and system code.

F. Electronic Mail (Email) Message: A message created or received on an electronic mail system such as Microsoft Outlook, or Gmail, including any attachments such as word processing and other electronic documents transmitted with the message, as well as calendar items. This does not include instant messages.

G. External Email Addresses: Email addresses not ending in "@fiscal.treasury.gov."

H. Federal Tax Information (FTI): Federal tax returns and return information, as defined by the Internal Revenue Code, at 26 U.S.C. § 6103. For more information on returns and return information, please see IRS Publication 1075.

I. Government Furnished: Resources owned or leased by the government provided for the accomplishment of official work. Resources include devices, software, and accounts.

J. Instant Messaging (IM): Near real-time text, voice, and/or video communications between individuals or groups. This includes, but is not limited to, instant messaging within an email client, text messaging, and chat messaging applications.

K. Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information linked or linkable to a specific individual. PII includes but is not limited to Privacy Act- protected information. The following are some examples of PII:

    a. Low Risk: name, email address, phone number, physical home address;
    b. Moderate Risk: date of birth, birth location, photograph;
    c. High Risk: social security number, bank account number, Federal Tax Information (FTI) with regard to individuals.

L. Privately-Owned Accounts: Resources not provided by the government that are purchased, leased, or licensed by someone or an organization other than the government. Resources include devices, software, and accounts. Personal email, IM, and social media accounts are considered privately owned.

M. Proprietary Controlled Business Processes: Sensitive and closely controlled business process and workflows where the disclosure of details could have severe or catastrophic impact on Fiscal Service's ability to achieve its mission.

N. Record: A document made or received to comply with a law or to conduct public business and is being preserved because it is evidence of Treasury policy, decisions, and business activities, or contains other information of value to the Federal Government.

O. Return: A return means any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of title 26 of the United States Code which is filed with the Secretary of the Treasury by, on behalf of, or with

respect to any person, and any amendment or supplement thereto, including supporting schedules, attachments or lists which are supplemental to, or part of, the return so filed. Examples of returns include forms filed on paper or electronically, such as Forms 1040, 941, 1099, 1120 and W-2.

P. Return Information: The term "return information" means—

1. A taxpayer's identity, the nature, source, or amount of their income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over assessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense,

2. Any part of any written determination or any background file document relating to such written determination (as such terms are defined in section 6110 (b)) which is not open to public inspection under section 6110,

3. Any advance pricing agreement entered into by a taxpayer and the Secretary, and any background information related to such agreement or any application for an advance pricing agreement, and

4. Any agreement under section 7121, and any similar agreement, and any background information related to such an agreement or request for such an agreement, but such term does not include data in a form which cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer. Nothing in the preceding sentence, or in any other provision of law, shall be construed to require the disclosure of standards used or to be used for the selection of returns for examination, or data used or to be used for determining such standards, if the Secretary determines such disclosure will seriously impair assessment, collection, or enforcement under the internal revenue laws.

Responsibilities

A. Chief Information Officer (CIO) serves as the authorizing official for Fiscal Service email and IM systems, assuming responsibility for the operation of the information systems and the information contained therein, at an acceptable level of risk.

B. Chief Security Officer (CSO) is responsible for:

1. Providing leadership and policy direction for the bureau's enterprise security program.

2. Preparing and distributing security policies, standards, and additional guidance, as

necessary, to implement and monitor the security program for Fiscal Service.

3. Providing authoritative advice on security protections for Fiscal Service assets.

4. Approving or delegating approval authority for the removal or transfer of sensitive information and equipment from bureau facilities or authorized locations.

C. Chief Privacy Officer (CPO) is responsible for:

1. Ensuring the implementation of information privacy protections, including compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act and consulting with the Chief Counsel, as necessary.

2. Providing authoritative advice on privacy protections for Fiscal Service information.

3. Approving or delegating approval authority for the removal or transfer of sensitive information and equipment from bureau facilities or authorized locations.

D. Chief Information Security Officer (CISO) is responsible for:

1. Providing leadership and policy direction for the bureau's information technology (IT) security program.

2. Preparing and distributing IT security policies, standards, and additional guidance, as necessary, to implement and monitor the Fiscal Service IT security program.

3. Providing authoritative advice on security protections for Fiscal Service IT systems.

4. Approving or delegating approval authority for the removal or transfer of sensitive information and equipment from bureau facilities or authorized locations.

E. Employees are responsible for:

1. Observing the policies and guidelines governing the use of email and IM.

2. Seeking information from supervisors and/or managers, the Chief Security Officer, or the Chief Information Security Officer in case of doubt or misunderstanding.

3. Reporting violations of this policy to the Fiscal Service IT Service Desk as a security incident for appropriate action.

Policy

A. Government-furnished email and IM accounts shall be used for conducting Fiscal Service business. Except in limited circumstances, privately-owned email or IM accounts shall not be used for Fiscal Service business. Any limited emergency exceptions to this policy must be approved in writing by a senior management official (Director or above).

   Once written approval of a limited emergency exception for the use of privately-owned accounts is obtained, records on a privately-owned account must be forwarded to Fiscal Service accounts for archiving. Specifically, employees must forward incoming and outgoing messages used to conduct Fiscal Service business from privately-owned accounts (with any attachments), or, with regard to IMs, copies of the messages, to their government-furnished email account within 72 hours of receiving or sending a message relating to Fiscal Service work on a privately-owned account. Non-records, such as spam, personal messages, etc., are not subject to this policy and should be deleted as soon as practicable

B. Employees must also forward incoming and outgoing text messages used to conduct Fiscal Service business from government-furnished cell phones to government-furnished email addresses within 72 hours of receiving or sending the messages. Non-records, such as spam, personal messages, etc., are not subject to this policy and should be deleted as soon as practicable

C. Government-furnished email and IM accounts are provided for official use. Government-furnished email and IM may be used for limited personal use consistent with the provisions contained within Treasury Directive 87-04 “Personal Use of Government Information Technology Resources.”

D. Government-furnished email and IM accounts should not be used to subscribe to personal social media sites or mailing lists.

E. Employees are expected to abide by the Fiscal Service Employee Conduct Policy while using Government-furnished email and IM systems.

F. Employees, contractors, fiscal agents, and financial agents shall not send email or IM messages containing Treasury information to non-government-furnished accounts, except as required for work-related communications to members of the public or other third parties or as otherwise provided in this policy.

G. The Fiscal Service email system encrypts messages within the system boundary without user interaction. In the event sensitive information needs to be encrypted to ensure confidentiality when sent externally, users should utilize bureau-approved encryption methods.

H. Below are information types that require special care in the email and IM systems:

1. **Controlled Unclassified Information**–

   a. **General**

      (1) CUI information may be created, sent, stored, and discussed on email and IM systems provided the items are not covered by additional policy constraints or further restricted in the CUI HIGH Risk Information and Personally Identifiable Information (PII) categories below.

      (2) Email or IM messages containing CUI information should not be sent without validating a recipient has a valid need to know.

   b. **Within Treasury and the Federal Reserve** –

      (1) CUI information sent to non-Fiscal Service accounts must be encrypted. Emails sent to the Department (Treasury), other Treasury bureaus, and the Federal Reserve will be encrypted by the Fiscal Service email system without explicit user interaction.

   c. **Outside of Fiscal Service, Treasury, or the Federal Reserve** –

      (1) CUI information should not be sent to non-Fiscal Service, Treasury, or Federal Reserve accounts without management prior approval from the respective Assistant Commissioner and CSO, CPO, CISO, or delegate. Management prior approval should be documented on a FS Form 7005, Removal of Sensitive Information and Equipment.

      (2) CUI information sent to non-Fiscal Service, Treasury, or Federal Reserve accounts must be encrypted. Encryption should utilize bureau-approved encryption methods.

   d. CUI received from Fiscal and Financial Agents – Fiscal and financial agents must encrypt CUI sent to Fiscal Service accounts using approved encryption methods.

2. **CUI HIGH Risk Information** - Email and Instant Messaging (IM systems shall not be used to communicate, internally or externally, CUI HIGH Risk Information. CUI HIGH Risk information is prohibited from being created, sent, received, stored, or discussed on email and IM systems.

3. **Personally Identifiable Information**

   a. **Low Risk** PII may be sent unencrypted internally to other Fiscal Service email addresses (i.e., addresses ending in @fiscal.treasury.gov). Low Risk PII sent to external (non-Fiscal Service) email addresses is not required to be encrypted; however, the sender should validate the context of the information to determine if encryption may be warranted. For example, a list of names of meeting attendees does not require encryption, but a list of names of emergency personnel should be encrypted.

   b. **Moderate Risk PII** may not be sent to external email addresses without prior approval from the respective Assistant Commissioner and CSO, CPO, CISO, or delegate, and proper safeguards. Proper safeguards include encryption and ensuring a

valid need to know. Management prior approval should be documented on a FS Form 7005.

c. **High Risk PII** may not be created, sent, received, stored, or discussed on email and IM systems without an approved acceptance of risk signed by the respective Assistant Commissioner and CIO, and proper safeguards. Proper safeguards include encryption and ensuring a valid need to know. Management prior approval should be documented on a FS Form 7005.

4. **Federal Tax Information (FTI)**

a. Federal Tax Information (FTI) may be created, sent, stored, and discussed on email and IM systems provided the recipient is authorized to receive the information per the provisions of Internal Revenue Code § 6103.
b. Emails that contain FTI should be properly labeled (e.g., email subject contains "FTI") to ensure the recipient is aware the message content contains FTI.
c. Email transmissions that contain FTI must be encrypted using bureau-approved encryption mechanisms.

I. **Records Retention** - Employees and contractors must ensure record information contained within email and IMs are retained in accordance with Fiscal Service's record retention policies. Non-records, e.g., Spam, personal messages, etc, are not subject to retention.

J. **Information Marking** - If CUI information, including PII, is contained in an email, it shall be marked by beginning the body of the email with "***CONTROLLED UNCLASSIFIED INFORMATION***."

K. **Email Signature Blocks** - Email users are expected to abide by the Fiscal Service Employee Conduct Policy and exercise professional judgment in the content of signature blocks. Tag lines or statements that could be offensive to others or reflect poorly upon Fiscal Service may not be included. Tag lines may not include the device or version of software running on handhelds.

L. **Bulk Email** - Email users shall not send bulk email without management prior approval from a Division Director or above. This would not apply to communication between NTEU and bargaining unit employees.

M. **Incoming Email** – Employees should encourage individuals sending incoming email with CUI information, including PII, to utilize encryption to protect the confidentiality of the information. Employees may send an encrypted email to an individual to allow the sender to respond in an encrypted manner.

N. **Incident Reporting** - All incidents regarding improper use of email or IM systems shall be reported as a security incident to the Fiscal Service IT Service Desk at 304-480-7777.

Quick Reference Guide

Below is a quick reference guide to provide more insight into the artifacts that are allowable and prohibited from being processed in email and IM systems. It is not intended to be a comprehensive list, but it does provide some additional guidance regarding what can and cannot be shared. Further questions can be referred to your supervisor, the Chief Information Security Officer, or the Chief Security Officer. Alternatives for sharing information that may not be shared via email or IM are available in the Fiscal Service Data Classification Standard.

Low Risk Data	Internal – Permitted External - Permitted	Information that if unprotected would not compromise the Fiscal Service mission or an individual's privacy. **Examples**: publicly available facts/information
CUI Non-PII Low Risk	Internal – Permitted External – Form 7005 & Safeguards	Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs. **Examples**: contracts and filled-in acquisition documents
CUI PII Low Risk	Internal – Permitted External – Form 7005 & Safeguards	Any information about an individual maintained by an agency that if compromised would harm the privacy of the individual. **Examples:** name, email address, phone number, physical home address
CUI PII Moderate& High Risk	Moderate Risk - Internal – Permitted; External – Form 7005 & Safeguards High Risk – Requires Risk Acceptance	Any information about an individual maintained by an agency that if compromised could significantly harm the finances and/or privacy of the individual. **Examples: Moderate**: date of birth, birth location, photograph; **High**: social security number, bank account number, Federal Tax Information (FTI)
CUI Non-PII Moderate Risk	Internal – Permitted External – Form 7005 & Safeguards	Any information, the loss, misuse, or unauthorized access to or modification of which could significantly affect the national interest or the conduct of Federal programs. **Examples**: system configuration baselines, System Security documentation for FIPS 199 Low and Moderate systems
CUI High Risk	Internal – Prohibited External - Prohibited	Any information, the loss, misuse, or unauthorized access to or modification of which could severely or catastrophically affect the national interest or the conduct of Federal programs. **Examples**: proprietary business processes, FIPS 199 high information (which could include PII), security architecture for critical systems, System Security documentation for FIPS 199 High systems
Classified	Internal – Prohibited External - Prohibited	Any information designated by Executive Order 12968 or successor orders to require protection against unauthorized disclosure and is marked to indicate its classified status. **Example:** confidential, secret, and top secret

Requires Cover Sheet and/or Media Marking

APPROVAL:

X Timothy E. Gribben

Digitally signed by Timothy E. Gribben
Date: 2024.08.18 18:59:11 -04'00'

Timothy E. Gribben, Commissioner
Bureau of the Fiscal Service